U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: MaaS360 Cloud Services
Date: March 16, 2017
Bureau/Office: Office of the Chief Information Officer
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street, NW, Mail Stop 7124S MIB, Washington, DC 20240

Section 1. General System Information

A. Is a PIA required?

☒ Yes, information is collected from or maintained on
☐ Members of the general public
☒ Federal personnel and/or Federal contractors
☐ Volunteers
☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

MaaS360 Cloud Services (MaaS360) is a major application that provides the Department of the Interior (DOI) with a consolidated cloud-based management platform for all of its mobile devices (iOS, Android, Windows) operated within the DOI environment. MaaS360 simplifies the management process by providing a consolidated portal environment for Bureau and Offices, to monitor and manage the configuration, inventory, and security settings across their mobile devices. MaaS360 provides the ability to push patches and update configurations on user devices without impacting the user or having to have the device physically present. Other than the MaaS360 client application which is loaded on each device the system does not impact the user experience and is transparent to users of DOI's mobile devices.

DOI has implemented the use and management of Personally Owned Equipment (POE) with implementation of the Secure Productivity Suite (SPS) secure container functionality. The container is an application that is added to POE which creates a secure encrypted partition on the personal device which is isolated from actions taken on the personal device. The container allows POE users to receive/send emails and edit DOI documents within the container. MaaS360 can be used to apply configurations to the container as well as remotely wipe the container, while the remaining portion of the POE device is unaffected.

C. What is the legal authority?

Federal and DOI requirements require that Agencies manage their mobile device inventories, to include configuration management, asset management, and security configurations.

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; The Clinger-Cohen Act, 40 U.S.C. 11101, et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3541 et seq.; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☒ Other: *Describe*

DOI has added the Secure Productivity Suite (SPS) secure container functionality to the MaaS360 system which allows DOI employees to securely utilize DOI email functionality on their personal mobile devices where authorized.

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000698; MaaS360 Cloud Services

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI-47, HSPD12: Logical Security Files, 72 FR 11040, March 12, 2007

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used

☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Credit Card Number
☐ Law Enforcement
☐ Education Information
☐ Emergency Contact
☐ Driver’s License
☐ Race/Ethnicity
☐ Social Security Number (SSN)
☐ Personal Cell Telephone Number
☐ Tribal or Other ID Number
☐ Personal Email Address
☐ Mother’s Maiden Name
☐ Home Telephone Number
☐ Child or Dependent Information
☐ Employment Information
☐ Military Status/Service
☐ Mailing/Home Address
☒ Other: *Specify the PII collected.*

User/Administrator work email addresses, Work Phone number, username, device owner, device name, DeviceID, Model/Type (iPhone/Android), and Operating System version.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☐ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☒ Other: *Describe*

DOI policy requires that all mobile devices operated within the DOI environment are enrolled and managed by MaaS360. Users may request a device through email or a bureau/office form, or may be issued a device from their organization depending on each bureau/office internal process. Once a device is issued to a user, it is enrolled into MaaS360 and receives the default security configuration policy. Maas360 regularly queries the device to validate that the configuration is still implemented and will provide a complete inventory of the device settings, including installed applications, configuration settings, hardware settings, and patch status.

POE: The secure container requires the installation of the MaaS360 application and the use of the employee's device ID as well as government email address. The MaaS360 container establishes a separate secure location on the POE where DOI information is stored (i.e.,email, contacts, calendar). When employees request mobile devices, as part of their request they are required to provide their name (first, last), which also constitutes their username. Once the device is enrolled it will synchronize information between the device and BisonConnect, DOI's email system, which includes their business contact information.

D. What is the intended use of the PII collected?

PII collected generally includes work-related information such as the username and official email address, and information on the user's device. This information is used to identify users, assign or enroll devices, and manage and secure mobile devices in accordance with Federal requirements and Departmental policies.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

MaaS360 is a Department-wide application. Each Bureau/Office Mobile Device Manager (MDM) administrator has access to their bureau/office Portal and has the ability to review accounts and devices assigned to their respective bureau/office.

The Container Portal is used to manage personal devices across all of DOI, access is limited to four DOI master administrators and one security personnel.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

IBM/Fiberlink contractors has access to information for the purpose of supporting the MaaS360 application.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Users voluntarily provide their username and official email address when they submit a request for a government-issued mobile device or for use of secure container for POE. Users consent to use of that information to issue and manage mobile devices issued to the user. For example, if a user refuses to provide a username when requested then the user will not be issued a mail enabled smart phone. Each bureau/office has internal procedures, forms and Rules of Behavior that cover the requirements and management of government-issued equipment so there are numerous methods that users may receive notice and opportunity to consent when requesting devices or equipment.

The POE Container is a voluntary program. DOI employees who wish to participate in the program must provide the required user and device information for device enrollment and consent to the use of that information to manage the use and security of DOI information.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Users are provided notice through the publication of this privacy impact assessment and the DOI-47, HSPD12: Logical Security Files system of records notice, 72 FR 11040, March 12, 2007.

☒ Other: *Describe each applicable format.*

Users who access the DOI network, information systems or equipment are provided a warning banner and are informed that they are subject to monitoring, and information provided from individuals may be monitored to ensure the authorized use and security of DOI information.

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse actions. Unauthorized or illegal use may subject you to prosecution.

Each bureau/office also has their own internal procedures, forms that cover requirements and management of government-issued equipment. These processes and forms may include bureau specific notice on the policies and requirements for acceptable use, expectation of privacy, and use of information collected for issuance and use of government-issued equipment. All employees are notified via Departmental policy, mandatory security awareness training, DOI Rules of Behavior and the DOI Warning Banner that employee use of government-issued equipment and the DOI network is subject to monitoring and information provided from individuals may be monitored to ensure the authorized use and security of DOI information.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data regarding the devices is manually generated through the MaaS360 portal. Data can be retrieved using many different criteria such as Device Name, Username, E-mail Address, Device type, Manufacturer, Model, Operating System, IMEI/MEID, Installed Date, Last Reported, Device ID, Platform Name, Mailbox Managed, and Managed status.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*

☒ No

Reports are produced based on specific device criteria and not based on individuals. Generally reports are pulled to identify the number of devices which meet a defined requirement (e.g., Number of devices running IOS 7, number of devices with Google Hangouts application). Reports are used in the daily operations and management of DOI's mobile device inventory. Reports are only shared internally with DOI MaaS portal administrators, IT security, and Bureau and Office IT managers. Reporting on user activity is not available within the system.

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Individuals participating in the secure container provide data (username, work email address) as part of the enrollment process. An accurate email address must be provided in order to receive the enrollment notification.

B. How will data be checked for completeness?

Individuals participating in the secure container provide data (username, work email address) as part of the enrollment process. An accurate email address must be provided in order to receive the enrollment notification.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Once the device is registered in MaaS the information is synchronized continuously between the device and the MaaS portal. The information is current as long as the user has an assigned device. In the event of termination, retirement or transferring to another job, the device will be wiped and all information removed from MaaS in accordance with policy and records retention requirements. Each Bureau/Office has established processes and procedures for the removal of accounts and devices.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

MaaS360 program records are maintained under the DOI Departmental Records Schedule 1 – Administrative bucket (DAA-0048-2013-0001-0013), which has been approved by the National Archives and Records Administration (NARA). These administrative and information technology records map to 1.4A1 Information Technology – System Maintenance and Use Records, and have a temporary disposition. Records are cut off when superseded or obsolete, and destroyed three years after cut-off. Some records may be maintained under DOI bureaus and offices records retention schedules and will be retained in accordance with those schedules as appropriate.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Data is maintained in the system as long as the user has the assigned device. Users who separate, retire, or are terminated will have their devices wiped using the MaaS console. All user data is removed from both the device and portal at that time in accordance with Departmental policy and records retention requirements. Each Bureau/Office has created individual processes and procedures for disposing of the data.

Users participating in the POE Container can remove the container at their discretion. Once the container is removed from the POE device all data is removed.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal privacy risk as the information maintained in the system is username and official email address for the purpose of managing and securing mobile devices in accordance with Federal and Departmental security requirements.

MaaS360 is a cloud-based software as a service mobile device management (MDM) application that operates outside the DOI Assessment and Authorization boundary. DOI recently awarded the contract to AT&T for use of the MaaS360 which is hosted in the cloud and managed by IBM/Fiberlink (www.fiberlink.com) with some administrative functions being performed by DOI administrative staff through a consolidated web-based portal. MaaS360 provides the ability to monitor devices and remotely wipe the device for security reasons. There are no physical components included in DOI's portion of the MaaS360 authorization boundary; controls consist of management and oversight capabilities. The administrative functions include user, device configuration, and security settings. The only interaction between MaaS360 and DOI is the validation of user devices and the enrollment into MaaS360 by administrators.

DOI has implemented the use and management of Personally Owned Equipment (POE) with implementation of the Secure Productivity Suite (SPS) secure container functionality. The container is an application that is added to POE which creates a secure encrypted partition on the personal device which is isolated from actions taken on the personal device. The container allows POE users to receive/send emails and edit DOI documents within the container. MaaS360 can be used to apply configurations to the container as well as remotely wipe the container, while the remaining portion of the POE device is unaffected. Information contained within the SPS container is encrypted and separate from other information stored on the POE. The container is configured to not allow transfer of data in or out of the container.

The secure container requires the installation of the MaaS360 application and the use of the employee's device ID as well as government email address. The MaaS360 container establishes a separate secure location on the POE where DOI information is stored (ie. Email, contacts, calendar). When employees request mobile devices, as part of their request they are required to provide their name (first, last), which also constitutes their username. Once the device is enrolled it will synchronize information between the device and DOI's email system BisonConnect, which includes their business contact information. System administrators can only access the the container configuration and the remote wipe capability of the system, they do not have access to the user's POE.

As the service provider, IBM/Fiberlink is responsible for the management and operation of the Cloud System as a Service (SaaS) managing the system configuration and ensuring that the appropriate security controls are implemented. As the cloud service provider IBM/Fiberlink administrators have access to all data contained within the cloud environment. IBM/Fiberlink administrators have undergone background investigations and per contract have no ownership to DOI data stored within the system.

DOI has the means to evaluate control descriptions, documentation, test results, and vulnerabilities that are identified. DOI devices are enrolled in the MDM solution to provide management and oversight of the devices. Communications between devices and the user interface to the management portal are encrypted using a FIPS 140-2 validated OpenSSL encryption module. DOI completed a System Security Plan to assesses the security controls for MaaS360 as part of the security authorization, and to meet requirements under the Federal Information Security Modernization Act of 2014 and National Institute of Standards and Technology (NIST). Continuous monitoring is conducted in conjunction by both the IBM/Fiberlink and DOI security team, and assessments are performed annually, and penetration testing and in-depth monitoring are conducted to ensure compliance with all vulnerability mitigation procedures. Also, the Maas360 Information System Security Officer reviews the system security plan annually or when needed to ensure that the system maintains compliance with security requirements.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The information maintained is necessary to properly manage and secure government-issued and voluntary participants using personally owned mobile devices in accordance with Federal requirements and Departmental policy.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable since the system does not derive new data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☐ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Device users do not have access to the MaaS360 console or system. System Administrators have access and their access is based on least privileges as required for official duties.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

AT&T is the contractor responsible for maintaining the system. MaaS360 is a cloud service and DOI only has limited access to the configuration and administration of the service. The DIAR (Department of the Interior) Clause 1452.224-1 “Privacy Act Notification (July 1996), Federal Acquisition Regulations (FAR) Clauses pertaining to the Privacy Act and Privacy or Security Safeguards are included in the contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*
☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Not applicable since information is not being collected as a function of monitoring individuals.

M. What controls will be used to prevent unauthorized monitoring?

Device criteria is monitored, individual user activity is not monitored within the system. However, controls in place to prevent unauthorized activity include access controls, least privileges, mandatory security and privacy training, DOI Rules of Behavior, and security audits to ensure compliance with Departmental security policy.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☐ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits

☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

MaaS360 is a System as a Service (SAAS) provided by IBM/Fiberlink and has been evaluated against the requirements established by FedRAMP and is continuously monitored by the vendor as well as DOI security personnel for potential lapses in security.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

IBM/Fiberlink as the Cloud Service Provider and AT&T as the contract manager are responsible under contract for maintaining the security and privacy of information contained within the system in accordance with FISMA, NIST Standards, and Privacy Act requirements. The MaaS360 System Owner is responsible for protecting the privacy of individuals for this application and for addressing Privacy Act requests or complaints in consultation with the Privacy Officer. Procedures for submitting Privacy Act requests or complaints are outlined in DOI Privacy Act Regulations at 43 CFR Part 2, Subpart K available at http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=43:1.1.1.1.2, and in the published Privacy Act system of records notice, DOI-47, HSPD12: Logical Security Files, which may be viewed on the DOI SORN website at: https://www.doi.gov/privacy/sorn.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Contractors and system administrators with access to the data are responsible for reporting any potential loss, compromise, unauthorized disclosure or unauthorized access of data. This responsibility is described in DOI security and privacy policies, mandatory IT security and privacy training, and DOI Rules of Behavior. The System Owner is responsible for ensuring proper use of the data and the requirements for reporting incidents.